DOCUMENTO DE SEGURIDAD DE

Antonio Gil de San Antonio

FECHA: 11 de febrero de 2014

1. INTRODUCCIÓN

El presente documento y sus anexos, que girarán bajo el nombre de “documento de seguridad de Antonio Gil de San Antonio“, se crea por Antonio Gil de San Antonio en cumplimiento de lo dispuesto por el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, LOPD), que establece que “*el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural*”.

En este sentido, el presente documento de seguridad recoge las medidas técnicas y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los sistemas de información de Antonio Gil de San Antonio, de conformidad con lo dispuesto por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en lo sucesivo, RLOPD).

Este documento de seguridad es único y comprensivo de todos los ficheros o tratamientos de Antonio Gil de San Antonio, y responde a las exigencias establecidas en relación a las medidas de seguridad de nivel básico, de conformidad con el tipo de datos que trata y/o almacena, reguladas en el título VIII del Reglamento de desarrollo de la LOPD.

Por otro lado, conviene tener presente que, tal y como estipula el artículo 88 del RLOPD, el documento de seguridad de Antonio Gil de San Antonio:

- Es de obligado cumplimiento para todo el personal con acceso a los sistemas de información que traten datos de carácter personal.
- Debe mantenerse en todo momento actualizado y debe ser revisado:
  - Siempre que se produzcan cambios que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas; como son la producción de cambios relevantes en:
    - los sistemas de información
    - el sistema de tratamiento empleado
    - la organización
    - el contenido de la información incluida en los ficheros o tratamientos
  - Como consecuencia de la realización de los controles periódicos determinados.
- Debe adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
- Tiene el carácter de documento interno de la organización, en todo caso.

2. ÁMBITO DE APLICACIÓN

El ámbito de aplicación del presente documento abarca todos los ficheros que contienen datos de carácter personal, referidos en el punto 5.1, que se hallan bajo la responsabilidad de Antonio Gil de San Antonio, así como los sistemas de información, soportes y equipos empleados para el tratamiento de dichos datos, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, y las personas que intervienen en el tratamiento y los locales en los que se ubican dichos ficheros.

Concretamente, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los que se indican a continuación:

NOMBRE DEL FICHERO	NIVEL DE SEGURIDAD
CLIENTES Y/O PROVEEDORES	Básico

2.1 Ámbito Subjetivo

El presente documento de seguridad pertenece a:

Antonio Gil de San Antonio
Calle Sacrificio, 21 5º D 28032 Madrid
(Madrid)
Correo-e: antonio.gils@hotmail.com
Telf.: 696320807
Fax:

2.2 Ámbito Objetivo. Recursos protegidos

Se entiende por recurso protegido "*cualquier parte componente del sistema de información* "; esto es, los ficheros referidos en el punto 5.1, así como los programas, soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal.

La descripción de los recursos protegidos se realiza, en el anexo II y el anexo IV del presente documento, individualizándola por ficheros y haciendo constar por cada uno de ellos su nombre, ubicación, breve descripción del contenido, finalidad de tratamiento y accesos, con identificación de los usuarios y/o perfiles que están autorizadas para acceder a los datos de carácter personal y, en su caso, la o las medidas de seguridad lógicas para garantizar la confidencialidad.

2.3 Definiciones

En este apartado del documento de seguridad se recogen las definiciones aplicables en materia de protección de datos de carácter personal conforme a lo dispuesto por el RLOPD.

Accesos autorizados	Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
Afectado o interesado	Persona física titular de los datos que sean objeto del tratamiento.
Autenticación	Procedimiento de comprobación de la identidad de un usuario.
Cancelación	Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
Cesión o comunicación de datos	Tratamiento de datos que supone su revelación a una persona distinta del interesado.
Consentimiento del interesado	Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
Contraseña	Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.
Control de acceso	Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
Copia de respaldo	Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
Dato disociado	Aquel que no permite la identificación de un afectado o interesado.
Datos de carácter personal	Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
Datos de carácter personal relacionados con la salud	Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Destinatario o cesionario	La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Documento	Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
Encargado del tratamiento	La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Exportador de datos personales	La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
Fichero	Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Ficheros de titularidad privada	Los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
Ficheros de titularidad pública	Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre público.
Fichero no automatizado	Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

Ficheros temporales	Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
Importador de datos personales	La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.
Identificación	Procedimiento de reconocimiento de la identidad de un usuario.
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
Persona identificable	Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
Perfil de usuario	Accesos autorizados a un grupo de usuarios.
Procedimiento de disociación	Todo tratamiento de datos personales que permita la obtención de datos disociados.
Recurso	Cualquier parte componente de un sistema de información.
Responsable del fichero o del tratamiento	Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Responsable de seguridad	Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
Sistema de información	Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
Sistema de tratamiento	Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
Soporte	Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Tercero	La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Transferencia internacional de datos	Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.
Transmisión de documentos	Cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
Tratamiento de datos	Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Usuario	Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

3. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES.

Los ficheros objeto de este documento de seguridad son accesibles únicamente por las personas que se identifican en el propio documento, teniendo, en su caso, acceso mediante red local en la propia entidad, o a través de red externa.

Solamente tienen acceso a los mismos las personas que han sido referidas e identificadas en los apartados "control de acceso lógico" y "control de acceso físico" del anexo II y con los controles de seguridad que han sido especificados.

En el anexo III se identifica al responsable de seguridad de Antonio Gil de San Antonio, encargado de gestionar los permisos de acceso de los usuarios, el procedimiento de asignación, distribución y almacenamiento que garantiza la confidencialidad e integridad y la forma de almacenar las contraseñas, durante su vigencia, para que resulten ininteligibles, así como la periodicidad con la que son cambiadas las palabras de paso, claves o contraseñas.

3.1 Control de acceso

De entre las obligaciones del personal de Antonio Gil de San Antonio, destaca el hecho de que únicamente deben acceder a aquellos datos y recursos que precisen para el desarrollo de sus funciones y, por tanto, a aquellos sobre los cuales se encuentren autorizados en el presente documento.

Antonio Gil de San Antonio se encarga de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, tal y como viene reflejado en el anexo II, bajo la denominación de “Control de acceso lógico”.

Asimismo, dispone de mecanismos para evitar que un usuario pueda acceder a recursos con distintos derechos de los autorizados. Mecanismos que, en caso de soportes informáticos, pueden consistir en la asignación de contraseñas para acceder a los mismos, y en caso de documentos, en la entrega de mecanismos de apertura de dispositivos de almacenamiento donde se recopile la información, tales como llaves.

La modificación de algún dato o información sobre la concesión, alteración, modificación, inclusión o anulación de los accesos autorizados y los usuarios que figuran en la relación correspondiente de este documento, ya referida, corresponde exclusivamente al personal autorizado en el anexo V.

En caso de que exista personal ajeno a Antonio Gil de San Antonio que tenga acceso a los recursos protegidos, este estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

3.2 Gestión de soportes y documentos

Los soportes y los documentos en los que se encuentran los ficheros son los especificados en el apartado "soportes y documentos" del anexo IV.

Los usuarios que traten o accedan a los soportes o documentos con datos de carácter personal son los encargados, en cada caso, de vigilar y controlar que personas no autorizadas no puedan acceder al soporte físico o documentos por ellos custodiados. Dichos usuarios autorizados se identifican en el anexo II del documento de seguridad.

Los soportes y documentos que contengan datos de carácter personal deben permitir identificar el tipo de información que contienen, ser inventariados y solo deben ser accesibles por el personal autorizado para ello en el presente documento, salvo que las características de los mismos imposibiliten la identificación en los términos indicados; en tal caso, quedará constancia motivada de ello en el documento de seguridad.

La identificación de los soportes y documentos que contengan datos de carácter personal que la organización considere especialmente sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento, debe ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad, tal y como se refleja en el anexo VI.

3.3 Ejecución del tratamiento fuera de los locales

En el supuesto de que se almacenen datos personales en dispositivos portátiles o se traten fuera de los locales del responsable de fichero, o del encargado del tratamiento, es preciso que exista una autorización previa por parte de Antonio Gil de San Antonio conforme a lo previsto en el anexo VI y, en todo caso, debe garantizarse el nivel de seguridad correspondiente al tipo de datos tratados.

3.4 Ficheros temporales, copias y reproducciones

Los ficheros temporales o copias de documentos que se creen exclusivamente para la realización de trabajos temporales o auxiliares deben cumplir el nivel de seguridad que le corresponda al fichero o documento original conforme a los criterios establecidos en la normativa sobre protección de datos de carácter personal.

Estos ficheros temporales o copias de trabajo son borrados o destruidos, de forma que se evite el acceso a la información contenida en los mismos o su recuperación posterior, una vez que han dejado de ser necesarios para los fines que motivaron su creación.

La generación de copias o la reproducción de documentos únicamente puede realizarse por el personal autorizado en el anexo II del documento de seguridad, o bajo su exclusivo control.

3.5 Responsable de seguridad

Antonio Gil de San Antonio ha designado uno o varios responsables de seguridad,

encargados de coordinar y controlar las medidas de seguridad definidas en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con la normativa sobre protección de datos de carácter personal.

3.6 Medidas Alternativas

Las medidas de seguridad respecto de las que Antonio Gil de San Antonio ha establecido un cumplimiento alternativo de las obligaciones establecidas por el RLOPD, por hallarse prevista dicha posibilidad en el citado texto legal, se regulan en el anexo IX de este documento.

3.7 Identificación y autenticación

Antonio Gil de San Antonio debe disponer de un sistema de seguridad informática que permita identificar y autenticar correctamente a los usuarios de los sistemas de información, de forma que se garantice que únicamente accederá a los ficheros el personal autorizado al efecto.

Asimismo, debe haber un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

La identificación debe ser llevada a cabo a través de un sistema concreto y único para cada uno de los usuarios que acceden a la información (nombre de usuario, identificación de empleado, nombre del departamento, etc.).

La nomenclatura a utilizar en la asignación de nombres de inicio de sesión para acceder al sistema de información es la definida en el anexo II.

La autenticación de los usuarios en los sistemas de Antonio Gil de San Antonio se realiza conforme al sistema descrito en el anexo II.

En este sentido, cuando el sistema de autenticación se base en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad e integridad.

Con el fin de garantizar la confidencialidad e integridad de las contraseñas, es recomendable que estas contengan un mínimo de ocho caracteres y vengan constituidas por mayúsculas, minúsculas, números y letras. La concreta política de contraseñas establecida por Antonio Gil de San Antonio se encuentra definida en anexo II.

Con el fin de garantizar la confidencialidad e integridad de las contraseñas, es recomendable que estas contengan un mínimo de 8 caracteres y vengan constituidas por mayúsculas, minúsculas, números y letras. Concretamente, la política de contraseñas establecida por Antonio Gil de San Antonio se encuentra definida en anexo II.

Del mismo modo, Antonio Gil de San Antonio velará porque se realice:

- El cambio de las contraseñas con la periodicidad establecida en el anexo II de este documento, que en ningún caso deberá ser superior a la mínima legalmente establecida; que es de 365 días.
- El almacenamiento de dichas contraseñas, mientras se hallen vigentes, de forma interna e ininteligible en el sistema informático.

3.8 Control de acceso físico

Los locales donde se encuentren ubicados los sistemas de información que contienen datos de carácter personal, deben ser objeto de especial protección, de manera que se garantice la confidencialidad e integridad de dichos datos, asimismo deben cumplir con las medidas de seguridad físicas correspondientes al soporte o documento en el que se encuentran dichos datos.

Antonio Gil de San Antonio debe poner en conocimiento del personal a su servicio, las obligaciones que les atañen, al objeto de proteger físicamente los soportes y documentos en los que se encuentran los ficheros y no permitir su manejo, utilización o identificación, por personas que no se encuentren autorizadas en el presente documento respecto al fichero de que se trate.

En el anexo II del presente documento se identifican los locales e instalaciones donde se ubican los ficheros, especificando sus características físicas y las medidas de seguridad física existentes.

Exclusivamente el personal autorizado en el presente documento podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información, en los términos descritos en el anexo II.

3.9 Procedimientos de realización de copias de respaldo y de recuperación de los datos

Antonio Gil de San Antonio ha establecido los procedimientos de actuación necesarios para la realización de copias de respaldo como mínimo semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Asimismo, se han establecido procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el presente documento.

Antonio Gil de San Antonio se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y

de recuperación de datos.

Todos los ficheros deben tener una copia de respaldo a partir de la cual se puedan recuperar los datos.

Los procedimientos de copia de respaldo y de recuperación de Antonio Gil de San Antonio se desarrollan en los términos que se indican en el anexo II.

Por otro lado, las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado, se realice una copia de seguridad previa a la realización de pruebas y se anote su realización en el presente documento.

3.10 Redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deben garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con el tratamiento de los datos de carácter personal y los sistemas de información de Antonio Gil de San Antonio deben actuar conforme a las funciones y obligaciones definidas y documentadas en el anexo V del presente documento.

Antonio Gil de San Antonio debe poner en conocimiento del personal a su servicio, las medidas y normas de seguridad que afectan al desarrollo de sus funciones, y las consecuencias de su incumplimiento, a través de cualquier medio de comunicación que garantice su recepción o difusión (intranet, correo electrónico, tablón de anuncios, etc.). Asimismo, debe poner a disposición del personal el presente documento de seguridad, de forma que puedan conocer la normativa de seguridad y las obligaciones que deben acatar en atención al perfil que ostentan.

Antonio Gil de San Antonio cumple con el deber de información indicado en el párrafo anterior mediante la inclusión de dichos extremos en los acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de los sistemas de información identificados en los anexos de este documento, así como mediante la remisión de una circular informativa a los mismos.

Las funciones y obligaciones del personal vienen determinadas con carácter general por el tipo de actividad que desarrollan en Antonio Gil de San Antonio, y con carácter específico por lo definido en el presente documento de seguridad, de modo que deben conocer y acatar su contenido en lo referente al fichero del que han sido considerados usuarios. En el anexo II se halla incluida la relación de los usuarios que tienen acceso a los recursos protegidos, así como los perfiles que acceden a los mismos.

En este sentido, y con carácter general, cuando un usuario trate soportes o documentos con datos de carácter personal debe vigilar y controlar que personas no autorizadas no puedan acceder al soporte físico o documentos por él custodiados.

Por otro lado, Antonio Gil de San Antonio ha delegado, en su caso, la realización de las funciones de control y/o las autorizaciones necesarias según la normativa sobre protección de datos, en las personas identificadas en el anexo VI del documento de seguridad.

5. FICHEROS CON DATOS DE CARÁCTER PERSONAL Y DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

En el presente apartado se identifican los ficheros de datos de carácter personal a los que se aplica el presente documento de seguridad.

La estructura de los ficheros de datos de carácter personal de los que Antonio Gil de San Antonio es responsable se halla contenida en el anexo I, el cual recoge las tablas esquemáticas resumen del contenido de las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos.

5.1 Ficheros

5.1.1 Como responsable del fichero

Los ficheros de los que Antonio Gil de San Antonio es responsable son los descritos en el anexo I del presente documento, los cuales se relacionan de forma sintética en la tabla siguiente:

NOMBRE DEL FICHERO	NIVEL DE SEGURIDAD
CLIENTES Y/O PROVEEDORES	Básico

Respecto de los ficheros incluidos en la tabla anterior debe verificarse el contenido del anexo VIII, en el que se identifican los encargados del tratamiento designados conforme al artículo 82 del RLOPD, en su caso, para el tratamiento de los mismos en las condiciones descritas en el citado anexo.

En este sentido, conviene tener presente que Antonio Gil de San Antonio identificará, como mínimo, los encargados del tratamiento, así como las condiciones del encargo, en el documento de seguridad.

Asismismo, el personal del encargado del tratamiento deberá comprometerse al cumplimiento de las medidas de seguridad previstas en el presente documento en relación al fichero de que se trate.

5.1.2 Como encargado del tratamiento

Los ficheros que Antonio Gil de San Antonio trata y/o almacena en sus propios locales como encargado del tratamiento de los datos de carácter personal responsabilidad de terceros, se identifican, en su caso, en el anexo VIII.

En el mismo anexo se detallan, a su vez, las condiciones del encargo, identificándose: el fichero o tratamiento respecto de los que Antonio Gil de San Antonio actúa como encargado del tratamiento, así como el responsable de tales ficheros o tratamientos, y las medidas de seguridad a implantar en relación con dicho tratamiento en función del nivel de seguridad asignado, en su caso, por el responsable.

5.2 Sistemas de Información

Los sistemas de información que tratan estos ficheros y, consecuentemente, los datos de carácter personal que en ellos se encuentran, son los que figuran en “Inventario de soportes y/o documentos” del anexo IV de este documento.

6. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

En el ámbito del presente documento de seguridad se entiende por incidencia, *cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos*, de modo que constituya o pueda constituir un riesgo para la confidencialidad, disponibilidad o integridad de los ficheros y/o de los datos de carácter personal que contienen.

En este sentido, en aras a garantizar la confidencialidad, disponibilidad e integridad de la información contenida en los ficheros cuya responsabilidad corresponde a Antonio Gil de San Antonio, de acuerdo con lo establecido en la normativa sobre protección de datos de carácter personal, se establece un procedimiento de gestión de incidencias con vistas a prevenir el peligro que representan para la seguridad de la información.

6.1 Procedimiento de notificación, gestión y respuesta ante incidencias.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento y/o consulta de datos de carácter personal en los ficheros objeto de este documento, deben tener conocimiento del procedimiento para actuar en caso de incidencia.

Dicho procedimiento se ha dado a conocer a través de los contratos suscritos en cada caso, y mediante la difusión de las funciones y obligaciones del personal al servicio de Antonio Gil de San Antonio. En dichos documentos se indican las siguientes instrucciones:

- Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad, disponibilidad o integridad de la información de la organización deberá comunicarlo inmediatamente al responsable de seguridad, con identificación clara del tipo de incidencia producida y su descripción detallada, en la que figurarán las intervenciones de personas que hayan podido tener relación con la producción de la incidencia, el momento -día y hora- en el que se ha producido, la persona que realiza la notificación de la incidencia, a quien se le comunica y los efectos que se hubieran derivado de la incidencia.
- Una vez comunicada la incidencia deberá solicitar al responsable de seguridad un acuse de recibo en el que se haga constar que ha recibido la notificación de la incidencia y que esta notificación contiene todos los requisitos descritos en el párrafo anterior.

6.2 Registro de incidencias

A estos efectos se crea un registro de incidencias en el anexo VII de este documento, gestionado bajo la responsabilidad del responsable de seguridad, en el que se hará constar:

- Tipo de incidencia
- Momento de su producción (fecha y hora)
- Persona que la notifica
- Persona a la que se comunica
- Efectos de la incidencia
- Medidas correctoras adoptadas, en su caso

Del mismo modo, también deberán consignarse los procedimientos realizados para la recuperación de los datos, indicando la persona que ejecuta el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. La ejecución de dichos procedimientos requiere de la autorización del responsable del fichero (cfr. anexo VI).

7. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN, Y REUTILIZACIÓN DE SOPORTES Y DOCUMENTOS

Antonio Gil de San Antonio siempre que deba desecharse cualquier documento –*original, copia o reproducción*- o soporte que contenga datos de carácter personal debe procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Del mismo modo, siempre que se proceda al traslado físico de documentación o de soportes, deben adoptarse las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información trasladada durante el transporte de la misma.

DISPOSICIÓN FINAL

El presente documento ha sido aprobado por Antonio Gil de San Antonio, como responsable de los ficheros, en fecha 11 de febrero de 2014 aceptándolo en su totalidad y ordenando su ejecución y cumplimiento, en particular por todos aquellos a quienes afecta y, en general, por todo el personal de Antonio Gil de San Antonio, para lo que se tomarán las medidas oportunas.

En Madrid, a 11 de febrero de 2014

Fdo. Antonio Gil de San Antonio

Anexo I.- CONTENIDO DE LAS SOLICITUDES DE INSCRIPCIÓN: ESTRUCTURA DE FICHEROS

FICHERO – CLIENTES Y/O PROVEEDORES

DATOS DEL FICHERO	
Nombre del fichero	**CLIENTES Y/O PROVEEDORES**
Descripción	**GESTION DE CLIENTES Y/O PROVEEDORES**
Finalidades y usos previstos	**Gestión Contable, Fiscal y Administrativa**

RESPONSABLE DEL FICHERO	
Denominación social	**Antonio Gil de San Antonio**
N.I.F.	**51400692Q**
Domicilio Social	**Calle Sacrificio, 21 5º D 28032 Madrid (Madrid)**
Teléfono	**696320807**
Fax	
Correo electrónico	**antonio.gils@hotmail.com**

ACCESO / RECTIFICACIÓN / CANCELACIÓN / OPOSICIÓN	
Nombre oficina o dependencia	**Antonio Gil de San Antonio**
N.I.F.	**51400692Q**
Dirección postal/Apdo. de correos	**Calle Sacrificio, 21 5º D 28032 Madrid (Madrid)**
Teléfono	**696320807**
Fax	
Correo electrónico	**antonio.gils@hotmail.com**

ENCARGADO DEL TRATAMIENTO	
Denominación social	
N.I.F.	
Dirección postal	
Teléfono	
Fax	
Correo electrónico	

PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA	
Origen y procedencia de los datos	**El propio interesado o su representante legal**
Colectivo o categoría de interesados	**Proveedores, Clientes y Usuarios**

ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS	
Carácter identificativo	**NIF / DNI, Nombre y apellidos, Dirección, Teléfono**
Datos especialmente protegidos	
Otros datos especialmente protegidos	
Otros datos tipificados	**Características Personales, Económicos, Financieros y de Seguros, Circunstancias Sociales, Información Comercial, Transacciones de Bienes y Servicios**

SISTEMA DE TRATAMIENTO
Automatizado

MEDIDAS DE SEGURIDAD	
Nivel de seguridad	**Básico**

COMUNICACIÓN DE DATOS	
Destinatarios / Categorías	**Bancos, Cajas de Ahorro y Cajas Rurales, Organizaciones o Personas Directamente Relacionadas Con El Responsable, Administración Tributaria**
Otros	

PERSONA FÍSICA QUE EFECTÚA LA NOTIFICACIÓN	
Nombre y Apellidos	**Juan Francisco Aguiar García**
N.I.F	**52342897A**
Cargo	**Adaptador LOPD**
Dirección profesional	**Calle Sacrificio, 21 5º D 28032 Madrid (Madrid)**
Teléfono	**696320807**

Anexo II.- DESCRIPCIÓN DE LOS FICHEROS Y MEDIDAS ESPECÍFICAS

FICHERO – CLIENTES Y/O PROVEEDORES

DESCRIPCIÓN DEL CONTENIDO

GESTION DE CLIENTES Y/O PROVEEDORES.

CONTROL DE ACCESO LÓGICO

Las funciones del personal de Antonio Gil de San Antonio con acceso a los datos de carácter personal están descritas en el anexo V del presente documento.

Los permisos de acceso se conceden, alteran o anulan por el responsable de seguridad o un usuario autorizado por este, teniendo en cuenta las funciones que deben desarrollar los usuarios conforme a su puesto de trabajo, tal y como se recoge en el anexo indicado en el párrafo anterior.

Los perfiles autorizados, con carácter general, para acceder a los datos y recursos asociados al fichero CLIENTES Y/O PROVEEDORES se identifican en la tabla siguiente:

PERFILES	DESCRIPCIÓN
Gerencia	Dirección de la Empresa

En la tabla siguiente se identifican los usuarios autorizados específicamente para acceder y tratar los datos y recursos asociados al fichero CLIENTES Y/O PROVEEDORES, en atención a su pertenencia a los perfiles indicados anteriormente y al tipo de tratamiento que pueden realizar:

Gerencia	
USUARIOS	**TIPO DE TRATAMIENTO**
Antonio Gil de San Antonio	Mixto

CONTROL DE ACCESO FÍSICO

Los equipos que dan soporte a los sistemas de información, y los dispositivos de tratamiento y/o almacenamiento de datos, se ubican en las áreas o lugares descritos a continuación:

	Sede principal
	TRATAMIENTO AUTOMATIZADO
DESCRIPCIÓN FÍSICA	Piso en la sede del responsable del fichero
MEDIDAS DE SEGURIDAD	Puerta de seguridad con alarma

Los usuarios indicados a continuación son los únicos autorizados para acceder a la sala de servidores:

- Antonio Gil de San Antonio

COPIAS DE RESPALDO Y PROCEDIMIENTO DE RECUPERACIÓN

El método seguido para realizar las copias de respaldo en relación con este fichero reúne las siguientes características:

Descripción:

Programación:

Por otro lado, en relación a los procedimientos de recuperación de datos, el responsable del fichero garantiza la reconstrucción íntegra de los datos mediante la comprobación del correcto funcionamiento de las copias de respaldo realizadas.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho.

SISTEMAS DE IDENTIFICACIÓN Y AUTENTICACIÓN

El **sistema de identificación** implantado por Antonio Gil de San Antonio consiste en: Contraseña.

El **sistema de autenticación** implantado por Antonio Gil de San Antonio está basado en el conocimiento de una contraseña o PIN. Los usuarios acceden a los sistemas de información mediante un sistema de autenticación basado en contraseñas.

El sistema de autenticación por contraseñas implantado, en su caso, por Antonio Gil de San

Antonio, tiene las siguientes características:

- **Longitud y contenido** de las contraseñas:
  - Deben tener una longitud mínima de 10 caracteres
  - Deben contener mayúsculas, minúsculas y números y símbolos
  - No existe un mecanismo que bloquee el acceso a los sistemas de información cada equis intentos reiterados de acceso no autorizado
  - Las contraseñas no caducan

Las contraseñas son asignadas, mediante un **procedimiento** interno, por el responsable de seguridad, y se distribuyen o comunican a los usuarios autorizados, evitándose que terceros no autorizados puedan llegar a conocerlas.

Las contraseñas se **almacenan** de forma ininteligible en los sistemas informáticos del responsable del fichero, garantizando su confidencialidad e integridad.

Anexo III.- RESPONSABLE DE SEGURIDAD

Antonio Gil de San Antonio ha designado un responsable de seguridad, encargado de coordinar y controlar las medidas de seguridad definidas en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con la normativa sobre protección de datos de carácter personal.

En este sentido, el responsable de seguridad designado es:

Antonio Gil de San Antonio

Anexo IV.- INVENTARIO DE SOPORTES

Nombre	TIPO DE SOPORTE O DOCUMENTO	DESCRIPCIÓN

Anexo V.- FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con el tratamiento de los datos de carácter personal y los sistemas de información de Antonio Gil de San Antonio tienen la consideración de usuarios y deben actuar conforme a las funciones y obligaciones definidas y documentadas en el presente anexo.

Los usuarios no deben tener acceso a los medios de procesamiento de la información hasta que hayan sido informados de sus obligaciones en relación al acceso y/o tratamiento de datos de carácter personal, y las consecuencias de su incumplimiento.

Las funciones y obligaciones del personal vienen determinadas con carácter general por el tipo de actividad que desarrollan en Antonio Gil de San Antonio, y con carácter específico por lo definido en el presente documento, de modo que deben conocer y acatar su contenido en lo referente al fichero del que han sido considerados usuarios. En el anexo II de este documento se halla incluida la relación de los usuarios que tienen acceso a los recursos protegidos, así como los perfiles que acceden a los mismos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por parte del personal al servicio de Antonio Gil de San Antonio, es sancionable conforme a la normativa aplicable a la relación jurídica existente entre el usuario y Antonio Gil de San Antonio (*laboral, funcionarial, etc.*).

Los usuarios se comprometen a adoptar y respetar los procedimientos de gestión de la seguridad de la información definidos en el documento de seguridad.

DEBER DE SECRETO

Esta obligación incumbe a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a ficheros que contienen datos personales.

El deber de secreto vincula a cuántas personas intervengan en el tratamiento de los datos, es decir, tanto a los usuarios como a los prestadores de servicios contratados.

En cumplimiento de esta obligación, los usuarios de Antonio Gil de San Antonio no pueden comunicar o revelar a terceros, datos que manejen o de los que tengan conocimiento en el desempeño de su cargo o funciones, y deben velar por garantizar la confidencialidad e integridad de la información que tratan.

El incumplimiento de esta obligación se tipifica como una falta grave en la normativa de protección de datos.

FUNCIONES DE CONTROL Y AUTORIZACIONES DELEGADAS

Antonio Gil de San Antonio puede delegar en otras personas la realización de las funciones de control y/o las autorizaciones previstas en la normativa sobre protección de datos de carácter personal.

Dichas delegaciones, en caso de existir, se hallan recogidas en el anexo VI del documento de seguridad, bajo el epígrafe “Delegación”.

OBLIGACIONES RELACIONADAS CON LAS MEDIDAS DE SEGURIDAD IMPLANTADAS.

Las obligaciones de los usuarios en materia de protección de datos personales consisten en:

- Acceder a los datos personales contenidos en los ficheros de Antonio Gil de San Antonio únicamente si se está autorizado y es necesario para el desempeño de sus funciones.
- No revelar información a personas ajenas a la organización, ni a usuarios no autorizados de la misma que no deban tener acceso a la información atendiendo a las funciones asignadas.
- Trabajar para mejorar la seguridad de la información, observando las normas y procedimientos de seguridad existentes.
- No realizar acciones que pudieran suponer un peligro para la seguridad de la información (p*. ej. introducción de software no autorizado por el responsable de seguridad, envío de información a través de correo electrónico sin las suficientes medidas de seguridad, conectar un módem a un ordenador que se encuentre conectado a la red corporativa, dejar información confidencial al alcance de cualquier persona, etcétera*).
- No sacar la información de las instalaciones de Antonio Gil de San Antonio sin estar debidamente autorizado, mediante soportes materiales o a través de cualquier medio de comunicación, salvo en los casos requeridos para el desarrollo de las funciones asignadas y, en todo caso, respetando lo establecido al respecto en este documento de seguridad y en los procedimientos establecidos a estos efectos por Antonio Gil de San Antonio.

- **Recursos y material de trabajo**

El uso de los recursos y de los materiales puestos a disposición de los usuarios por Antonio Gil de San Antonio debe orientarse al cumplimiento de las finalidades previstas para la ejecución de las funciones que les han sido encomendadas. Por tanto, no se autoriza la utilización de dichos recursos o materiales con fines personales o ajenos a los objetivos propios del puesto de trabajo correspondiente.

En el caso de que existan periféricos o dispositivos extraíbles que permitan grabar y/o almacenar datos, no deben utilizarse para grabar o almacenar información con fines personales. Asimismo debe evitarse, en la medida de lo posible, la utilización de este tipo de dispositivos para evitar la posible salida incontrolada de información de las instalaciones de Antonio Gil de San Antonio.

No obstante, en supuestos en que por motivos justificados de trabajo se requiera la salida de este tipo de soportes de las instalaciones de Antonio Gil de San Antonio, deberá

comunicarse esta circunstancia al responsable de seguridad, quien decidirá autorizarla o no y registrará, en su caso, la pertinente salida.

- **Uso de impresoras, escáneres y otros dispositivos de copia**

En caso de que se utilicen dispositivos de copia, como impresoras o fotocopiadoras, debe procurarse que, tras la impresión o fotocopia del documento, se proceda a la recogida inmediata de la copia, asegurándose de no dejar documentos o copias en las bandejas del dispositivo.

- **Gestión de incidencias**

Se entiende por incidencia cualquier anomalía que pueda producirse y suponer un peligro o afectar a la seguridad de los datos de carácter personal, entendida en su triple vertiente: confidencialidad, integridad y disponibilidad.

Constituye una obligación de los usuarios notificar a Antonio Gil de San Antonio, a través del responsable de seguridad, las incidencias de seguridad de las que tengan conocimiento de conformidad con el procedimiento establecido en esta política.

Los usuarios deben tener en cuenta, entre otras, las siguientes incidencias:

- La caída del sistema de la seguridad informática, por cualquier causa, que posibilite el acceso a los datos a personales por personas no autorizadas.
- El intento no autorizado de salida de un soporte.
- La destrucción total o parcial de soportes físicos que contengan datos personales.
- El cambio de ubicación física de ficheros de datos personales.
- Los intentos de acceso no autorizados o fallidos a ficheros con datos de carácter personal.
- El conocimiento por terceros del identificador de usuario o clave de acceso al sistema.
- La modificación de datos por personal no autorizado o desconocido.
- La pérdida de información.
- La existencia de sistemas de información sin las debidas medidas de seguridad.

Ante la producción de cualquiera incidencia, el usuario debe comunicar inmediatamente su producción al responsable de seguridad, el cual se encargará de su gestión y resolución.

En este sentido, el usuario debe rellenar la plantilla recogida en el anexo II de la política de seguridad de Antonio Gil de San Antonio, y remitirla a la cuenta de correo electrónico del responsable de seguridad, quien recibirá las notificaciones de incidencias y procederá a su registro, comunicándolas, a su vez, a los técnicos internos o externos encargados de la seguridad del sistema.

El conocimiento y la no notificación de la producción de una incidencia por parte de un usuario se considera como una falta contra la seguridad de los ficheros de Antonio Gil de San Antonio.

- **Gestión de soportes**

Se entiende por soporte, todo objeto físico que almacena o contiene datos o documentos u

objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

En este sentido, y con carácter general, cuando un usuario utilice soportes o documentos con datos de carácter personal debe, en cumplimiento del deber de custodia que le obliga, vigilar y controlar que no accedan a estos personas no autorizadas.

Únicamente los usuarios autorizados en el documento de seguridad pueden realizar copias o reproducciones, temporales o auxiliares, de documentos que contengan datos de carácter personal. Las copias o reproducciones realizadas deben destruirse o eliminarse, cuando dejen de ser necesarias para el fin que motivó su creación, de forma que se garantice que la información contenida en los estas no es accesible tras la destrucción o eliminación.

Los soportes, que contienen ficheros con datos personales, deben identificar la información que contienen mediante algún sistema de etiquetado y ser inventariados. En caso de que la información esté clasificada con nivel de seguridad alto el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a tratar dicha información.

Los soportes o documentos deben almacenarse en lugares de acceso restringido a los usuarios autorizados para tratar la información contenida en los mismos. En este sentido, con carácter general, debe evitarse: el uso de dispositivos de almacenamiento (*armarios, cajones...)* sin llave o sistemas equivalentes que dificulten o controlen su apertura; dejar sin custodia los soportes o documentos en la superficie de las mesa de trabajo o en lugares/áreas de acceso libre a personas no autorizadas.

Antonio Gil de San Antonio prohíbe que los soportes o documentos se ubiquen o sitúen fuera de los lugares previstos para su custodia o almacenamiento cuando no se estén utilizando.

Los soportes que vayan a ser retirados, destruidos o reutilizados deben ser borrados, de forma que se impida la recuperación posterior de la información que almacenan. Este mismo deber de destrucción se aplica a la información contenida en formato papel.

La salida de soportes con datos personales de las instalaciones autorizadas para su tratamiento y/o almacenamiento, debe ser previamente autorizada por Antonio Gil de San Antonio y debe constar en el documento de seguridad, identificando los usuarios autorizados y la vigencia de la autorización. La salida de soportes debe comunicarse al responsable de seguridad, quien verificará la autorización y registrará, en su caso, la salida.

• Terminales de trabajo y portátiles

Cada usuario es responsable de su puesto y/o estación/terminal de trabajo. Por tanto, cuando un usuario se ausente -*aunque sea temporalmente*- de su puesto de trabajo, de forma que no pueda controlar quien accede al mismo (*p. ej. para mantener una reunión, para ir a comer, etc.*), debe bloquear la estación/terminal de trabajo para impedir que pueda visualizarse la información de la pantalla o acceder a los datos con los que se estaba trabajando.

El bloqueo de la estación/terminal de trabajo puede llevarse a cabo mediante la activación

de un protector de pantalla, protegido con una contraseña, que impida la visualización de los datos. El desbloqueo de la estación/terminal de trabajo implicará la desactivación de la pantalla protectora mediante la introducción de la contraseña por el usuario.

Al finalizar la jornada de trabajo, cada usuario es responsable de apagar su equipo de trabajo. Los equipos deben apagarse completamente ya que en caso contrario, si algún fichero de la red quedara abierto, el proceso de copia de seguridad no lo incluiría y dicho fichero no tendría copia de respaldo en caso de producirse alguna incidencia.

Los ordenadores portátiles, por su parte, deben mantenerse siempre controlados para evitar su sustracción o pérdida, y deben disponer de las medidas de seguridad necesarias para garantizar la seguridad de la información que se trate en los mismos. La información tratada en este tipo de dispositivos debe volcarse en una carpeta de red, con las medidas de seguridad apropiadas, cuando vayan a dejar de utilizarse dichos dispositivos y, a continuación, debe eliminarse de los mismos.

• Uso de Internet y correo electrónico

Tanto el envío de información, por cualquier medio de comunicación electrónica, como la utilización de internet por parte del personal de Antonio Gil de San Antonio se encuentra exclusivamente limitada al desempeño de las actividades laborales o profesionales que corresponden a cada usuario. No se permite el uso de los medios o herramientas indicados para finalidades distintas a las mencionadas anteriormente.

Antonio Gil de San Antonio podrá inspeccionar los medios de producción *(correo electrónico, terminal de trabajo, portátil, PDA, tablet o cualquier otros soporte inventariado.)* facilitados a los empleados para el desempeño de sus funciones, en orden a verificar el correcto cumplimiento de sus obligaciones.

• Salvaguarda y protección de las contraseñas personales

Todos los usuarios de los sistemas de información utilizados en Antonio Gil de San Antonio deben disponer de contraseñas asociadas a sus identificaciones de usuario para permitirles el acceso a los mismos. Los identificadores y contraseñas proporcionados son personales e intransferibles. Cada usuario solo debe tener acceso a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones dentro de la organización.

Es necesario que el usuario, en su primer acceso al sistema o a una aplicación, cambie la contraseña que le ha sido asignada al ser dado de alta o, como consecuencia, de la ejecución del procedimiento de restauración de contraseña por cualquier causa. En caso de que sea necesario ejecutar el procedimiento de restauración de contraseñas, el usuario debe comunicárselo al administrador del sistema.

La vigencia de las contraseñas se establece en el documento de seguridad. La contraseña deberá modificarse al finalizar el término indicado en el documento de seguridad, salvo que por razones de seguridad sea necesario o conveniente hacerlo antes (*p. ej. porque se ha visto comprometida la contraseña del usuario*).

El usuario puede elegir la contraseña que desee, pero se recomienda no seleccionar como

contraseña palabras en cualquier idioma o códigos de valores asociable al usuario (*nombre de personas, matrículas, teléfonos, fechas, etc*.), permutaciones sencillas (*123456, 0000...*) o secuencias de teclado (*qwerty, asdfg...)*, ni utilizar en los cambios de contraseñas secuencias lógicas fácilmente deducibles.

Se prohíbe la divulgación o comunicación de la clave de acceso o contraseña a otras personas o usuarios, pertenezcan o no a la plantilla de Antonio Gil de San Antonio.

En caso de que el identificador de usuario o la clave de acceso fuera conocida fortuita o fraudulentamente por personas no autorizadas, debe comunicarse inmediatamente esta incidencia al responsable de seguridad, para proceder a su cambio según lo descrito anteriormente.

- **Copias de respaldo y recuperación de datos**

Toda la información debe gestionarse desde, y almacenarse en, el directorio de red correspondiente; no en los discos duros de los ordenadores de los usuarios.

Esta medida es necesaria porque las medidas de seguridad necesarias para garantizar la seguridad de la información se aplican a la información almacenada en el directorio de red (no en los ordenadores de los usuarios). De esta forma, la información indicada se incluirá en las copias de respaldo realizadas en la organización.

Anexo VI.- DELEGACIONES Y AUTORIZACIONES

AUTORIZACIÓN PARA EL TRATAMIENTO FUERA DE LOS LOCALES DE UBICACIÓN DEL FICHERO

En cumplimiento de lo dispuesto por el artículo 86 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, se **AUTORIZA** expresamente mediante el presente documento la realización del tratamiento de datos de carácter personal, relativo a ficheros cuya responsabilidad corresponde a Antonio Gil de San Antonio, fuera de los locales donde se hallan ubicados dichos ficheros, respecto de los siguientes usuarios o perfiles de usuarios:

- Antonio Gil de San Antonio

El ámbito de la presente autorización, se entiende incluido tanto el tratamiento fuera de los locales del responsable del fichero como del encargado del tratamiento, así como el almacenamiento de datos de carácter personal en dispositivos portátiles, que en función del nivel de seguridad, deberán ir cifrados.

Los usuarios o perfiles autorizados para tratar datos fuera de los locales, deben: guardar secreto de la información a la que accedan y garantizar el nivel de seguridad de los ficheros tratados en las condiciones descritas en el presente documento.

La presente autorización empezará a regir en la fecha indicada en la disposición final del documento de seguridad y permanecerá en vigor mientras la relación laboral, contractual o mercantil de la que trae causa reste vigente. Asimismo, finalizará la validez de la presente autorización en caso de que se acuerde la modificación o derogación expresa de la misma, elaborándose un nuevo documento de seguridad con tal fin.

AUTORIZACIÓN PARA LA SALIDA DE SOPORTES Y/O DOCUMENTOS

En cumplimiento de lo dispuesto por el artículo 86 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, se **AUTORIZA** expresamente mediante el presente documento la salida de soportes y documentos que contienen datos de carácter personal, relativos a ficheros cuya responsabilidad corresponde a Antonio Gil de San Antonio, fuera de los locales bajo el control del responsable del tratamiento, en los términos indicados a continuación:

USUARIOS AUTORIZADOS
Antonio Gil de San Antonio

Los usuarios o perfiles autorizados para sacar soportes y/o documentos deben: guardar secreto de la información a la que accedan y garantizar el nivel de seguridad de los ficheros tratados en las condiciones descritas en el presente documento.

La presente autorización empezará a regir en la fecha indicada en la disposición final del documento de seguridad y permanecerá en vigor mientras la relación laboral, contractual o mercantil de la que trae causa reste vigente. Asimismo, finalizará la validez de la presente autorización en caso de que se acuerde la modificación o derogación expresa de la misma, elaborándose un nuevo documento de seguridad con tal fin.

AUTORIZACIÓN PARA LA RECUPERACIÓN DE LOS DATOS

En cumplimiento de lo dispuesto por el artículo 100 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, se **AUTORIZA** expresamente mediante el presente escrito la utilización de las copias de respaldos realizadas conforme al presente documento de seguridad, con la finalidad de que se reconstruya la información y los datos al estado en el que se encontraban al tiempo de producirse su pérdida o destrucción, a los usuarios siguientes:

La presente autorización empezará a regir en la fecha indicada en la disposición final del documento de seguridad y permanecerá en vigor mientras la relación laboral, contractual o mercantil de la que trae causa reste vigente. Asimismo, finalizará la validez de la presente autorización en caso de que se acuerde la modificación o derogación expresa de la misma, elaborándose un nuevo documento de seguridad con tal fin.

Anexo VII.- REGISTRO DE INCIDENCIAS

REGISTRO DE INCIDENCIAS	
FECHA/HORA:	
TIPO DE INCIDENCIA	
DESCRIPCIÓN	
EFECTOS	
MEDIDAS CORRECTORAS	
EMISOR DE LA NOTIFICACIÓN	
RECEPTOR DE LA NOTIFICACIÓN	

PERSONA QUE EJECUTA EL PROCESO DE RECUPERACIÓN	
DATOS RESTAURADOS	
DATOS GRABADOS MANUALMENTE	

Anexo VIII.- PRESTACIONES DE SERVICIOS CON ACCESO A DATOS

ENCARGADOS DEL TRATAMIENTO

Antonio Gil de San Antonio ha contratado los servicios de terceros que implican el acceso y/o tratamiento de datos de carácter personal de los que es responsable en los términos que se describen a continuación:

LAMACOBA APM, S.L.	
IDENTIFICACIÓN DEL CONTRATO	**CONDICIONES DEL ENCARGO**
Contrato, de fecha 03 de febrero de 2014 con código de referencia CADET00001	Antonio Gil de San Antonio ha contratado a LAMACOBA APM, S.L. para la prestación de servicios, consistentes en Adaptación LOPD. El desarrollo de estos servicios implica el tratamiento de los siguientes ficheros: CLIENTES Y/O PROVEEDORES La vigencia del presente encargo viene determinada por la duración de los servicios contratados, descritos en el párrafo anterior La prestación de los servicios indicados se realiza: - En locales propios de LAMACOBA APM, S.L. - En locales propios de Antonio Gil de San Antonio Dicha prestación puede implicar/implica la incorporación de los datos en sistemas o soportes del encargado del tratamiento
Inferis Sistemas de Comunicación, S.L.	
IDENTIFICACIÓN DEL CONTRATO	**CONDICIONES DEL ENCARGO**
Contrato, de fecha 03 de febrero de 2014 con código de referencia CADET00002	Antonio Gil de San Antonio ha contratado a Inferis Sistemas de Comunicación, S.L. para la prestación de servicios, consistentes en Diseño, mantenimiento y producción de la página web. El desarrollo de estos servicios implica el tratamiento de los siguientes ficheros: CLIENTES Y/O PROVEEDORES La vigencia del presente encargo viene determinada por la duración de los servicios contratados, descritos en el párrafo anterior La prestación de los servicios indicados se realiza: - En locales propios de Inferis Sistemas de Comunicación, S.L. Dicha prestación puede implicar/implica la incorporación de los datos en sistemas o soportes del encargado del tratamiento

LOGISTICA INTEGRAL 2010, S.L.	
IDENTIFICACIÓN DEL CONTRATO	**CONDICIONES DEL ENCARGO**
Contrato, de fecha 03 de febrero de 2014 con código de referencia CADET00003	Antonio Gil de San Antonio ha contratado a LOGISTICA INTEGRAL 2010, S.L. para la prestación de servicios, consistentes en Transporte de materiales de venta a los clientes. El desarrollo de estos servicios implica el tratamiento de los siguientes ficheros: CLIENTES Y/O PROVEEDORES La vigencia del presente encargo viene determinada por la duración de los servicios contratados, descritos en el párrafo anterior La prestación de los servicios indicados se realiza: - En locales propios de LOGISTICA INTEGRAL 2010, S.L. - En locales propios de Antonio Gil de San Antonio Dicha prestación puede implicar/implica la incorporación de los datos en sistemas o soportes del encargado del tratamiento

CON EMPRESAS CLIENTE

Antonio Gil de San Antonio no presta servicios que impliquen el acceso y/o tratamiento de datos de carácter personal de terceros en los locales descritos en este documento de seguridad.

Anexo IX.- CONTROLES PERIÓDICOS

Antonio Gil de San Antonio verificará el cumplimiento de lo dispuesto en el presente documento de seguridad, de conformidad con los procedimientos y controles periódicos previstos en este anexo.

En este sentido, realizará las comprobaciones, según la periodicidad indicada, detalladas en la tabla siguiente:

		CONTROLES		
		REGULACIÓN	***DESCRIPCIÓN***	
PERIODICIDAD	***MENSUAL***	Control de acceso (art. 91 RLOPD)	*Relación actualizada de usuarios y perfiles, y accesos autorizados*	
		Autorizaciones (arts. 84, 86, 89, 92, 99, 100 y 112 RLOPD)	*Relación actualizada de autorizaciones y delegaciones*	
	TRIMESTRAL	Registro de incidencias (arts. 90 y 100 RLOPD)	*Análisis incidencias producidas y eficacia del procedimiento de resolución*	
	SEMESTRAL	Gestión de soportes (arts. 92, 97 y 101 RLOPD)	*Revisión del Inventario actualizado. Análisis del registro de entradas y salidas*	
		Copias de respaldo y recuperación* (arts. 94 y 102 RLOPD)	*Verificación eficacia procedimientos de copia de respaldo y recuperación*	
	ANUAL	Identificación y autenticación* (art. 93 RLOPD)	*Verificar cambio de contraseñas efectuado*	

Los controles señalados con el símbolo * son obligatorios de conformidad con los artículos citados en la tabla anterior; el resto de controles que se indican son recomendables para cumplir con las prescripciones establecidas por el artículo 88.7 del RLOPD.

El resultado de los controles practicados se adjuntará al presente documento de seguridad como parte de este anexo.

Anexo X.- MEDIDAS ALTERNATIVAS

No se han implementado medidas alternativas para el cumplimiento de las medidas de seguridad establecidas por la normativa sobre protección de datos.